OUCH!

SANS SECURITY AWARENESS

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Anda Adalah Sasaran

Pengenalan

Ramai orang beranggapan mereka bukan sasaran penyerang siber, dan bahawa sistem atau akaun mereka tidak mempunya apa-apa nilai. Ini adalah tidak benar. Jika anda menggunakan teknologi dalam apa juga keadaan, di tempat kerja atau di rumah, percayalah, kepada penjenayah anda mempunyai nilai. Bagaimanapun anda bernasib baik. Perlindungan terbaik bagi menentang serangan siber adalah diri anda sendiri.

Kenapa Anda Menjadi Sasaran

Terdapat berbagai jenis serangan siber di dalam Internet hari ini, dan semuanya mempunyai motivasi tersendiri. Jadi mengapa mereka mahu menyerang anda? Ini kerana dengan menggodam anda mereka telah mencapai matlamat mereka. Berikut adalah dua contoh serangan siber dan mengapa mereka mahu menyasar anda.

⚠ **Penjenayah Siber:** Mereka ini mahu mendapatkan sebanyak mungkin duit. Apa yang menjadikan Internet sangat berharga adalah mereka boleh menyasarkan semua orang di dunia hanya dengan menekan satu butang. Terdapat banyak cara untuk mereka mendapatkan duit anda. Sebagai contoh mencuri duit dari bank atau akaun persaraan, mencipta kad kredit dan menghantar bil kepada anda, menggunakan komputer anda untuk menggodam komputer lain, atau menggodam akaun media sosial atau akaun permainan video dan menjualnya kepada penjenayah lain. Terlalu banyak cara yang boleh penjenayah gunakan untuk mendapatkan duit anda. Ribuan penjenayah siber ini cuba menggodam seramai mungkin orang setiap hari termasuklah anda.

☆ **Penyerang Bersasar:** Mereka ini adalah dari golongan yang sangat terlatih, selalunya bekerja untuk kerajaan, sindiket penjenayah atau pesaing yang menyasarkan anda di tempat kerja. Anda mungkin beranggapan bahawa kerja anda tidak menarik banyak minat, tetapi jangan terkejut.

- Maklumat yang anda gunakan di tempat kerja mempunya nilai yang tinggi kepada syarikat atau kerajaan asing.
- Penyerang bersasar mungkin menyerang anda di tempat kerja bukan kerana mereka mahu menggodam anda tetapi untuk menggodam rakan sejawat atau sistem lain.

- **Penjenayah sebegini mungkin akan menjadikan anda sebagai sasaran kerana kerjasama yang anda jalinkan bersama syarikat atau rakan kongsi lain.**

Saya Selamat, Saya Mempunyai Anti-Virus

Saya sekarang adalah sasaran, tiada masalah. Saya hanya perlu memasang anti-virus dan tembok api pada komputer dan saya selamat, kan? Malangnya tidak. Kebanyakan orang beranggapan setelah mereka memasang peralatan keselamatan dan mereka kini selamat. Malangnya ini tidak betul.. Penyerang siber semakin hari semakin licik dan kebanyakan cara serangan yang mereka gunakan sekarang ini dapat mengelak teknologi keselamatan dengan mudah. Sebagai contoh mereka sentiasa mencipta perisian hasad yang tidak dapat dikesan oleh antivirus anda. Mereka mengelak tapisan e-mel anda dengan serangan phishing, atau menelefon dan cuba memperdaya kad kredit, duit atau kata laluan anda. Teknologi memainkan peranan penting untuk melindungi seseorang tetapi akhirnya anda sendiri adalah perlindungan terbaik.

Mujurlah tidak susah untuk kekal selamat. Akal fikiran dan tingkah laku asas menjadi pendinding terbaik anda. Jika anda mendapat e-mel, pesanan atau panggilan telefon yang terlalu mendesak, pelik atau mencurigakan, ia mungkin suatu bentuk serangan. Untuk memastikan komputer dan peranti anda selamat pastikan ianya dikemas kini dan bolehkan kemas kini automatik. Akhir sekali, gunakan ungkapan laluan yang kukuh dan unik untuk setiap akaun anda. Pertahanan terbaik anda adalah dengan mengambil tahu perkara berkaitan siber. Tidak pasti nak mulakan di mana? Pertimbangkan untuk melanggan surat berita bulanan OUCH! Di sans.org/ouch

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Editor Jemputan

Matt Bromiley *(@mbromileyDFIR) merupakan pakar forensik digital dan pasukan bertindak insiden. Beliau mempunyai lebih 8 tahun pengalaman dan telah berkhidmat dengan banyak organisasi dan menangani insiden di serata dunia. Matt juga merupakan pengajar kursus Forensik Digital dan Tindak Balas Insiden SANS FOR508 dan FOR572.*

SANS SECURITY AWARENESS

Sumber

Hentikan Perisian Hasad:	https://www.sans.org/u/L1J
Kejuruteraan Sosial:	https://www.sans.org/u/L1O
Penipuan Panggilan Telefon:	https://www.sans.org/u/L1T
Ungkapan Laluan:	https://www.sans.org/u/L1Y
Poster – Anda adalah sasaran:	https://www.sans.org/u/L23